

**IN THE UNITED STATE DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

ALEXYS TAYLOR, INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY SITUATED,

Plaintiffs,

v.

ALCON VISION, LLC

Defendant.

)
)
)
) Case No.: 1:21-cv-4019
)
)
) Judge: Robert M. Dow
)
)
)

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Alexys Taylor, (“Plaintiff”), brings this Amended Class Action Complaint individually and on behalf of all other similarly situated individuals against Defendant Alcon Vision, LLC (hereinafter “Alcon” or “Defendant”) to stop Defendant’s unlawful collection, use, storage, and disclosure of Plaintiff’s and the proposed Class’s sensitive, private, and personal biometric data. Plaintiff alleges the following upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief including investigation conducted by their attorneys. Further, Plaintiff alleges as follows:

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff Alexys Taylor is an individual citizen of the State of Indiana, who encountered the Defendant’s website while she was a citizen of Illinois and residing in Cook County, Illinois.

2. Defendant Alcon Vision, LLC is a Delaware limited liability company with its principal place of business in Fort Worth, Texas. It is registered to do business in Illinois with the Illinois Secretary of State.

3. Alcon Vision, LLC is a limited liability company whose sole member is CIBA Vision, LLC. CIBA Vision, LLC is a Delaware Limited Liability Company whose sole member is Alcon

Laboratories, Inc. Alcon Laboratories, Inc. is a Delaware corporation with its principal place of business in Fort Worth, Texas.

4. Defendant Alcon Vision, LLC may be served through its registered agent, Illinois Corporation Service, 801 Adlai Stevenson Drive, Springfield Illinois, 62703.

5. Jurisdiction is proper in this Court as the damage endured by Plaintiff occurred in Illinois, and Defendant operates its business in Illinois, targets business activity in Illinois, and purposefully avails itself of the laws, protections, and advantages of doing business in Illinois, with Illinois users like Plaintiff.

6. Venue is proper in this court pursuant to 735 ILCS 5/2-101 as, upon information and belief, Defendant does business in this county.

INTRODUCTION

7. Alcon is an eye care device company that sells eye care products, including contacts and eye glasses.

8. Alcon manufactures technology that allows customers to virtually try on their products.

9. Alcon also operates a website, myalcon.com (the “Website”), which *inter alia* allows customers to virtually try-on “color enhancement” contacts—allowing users to see how they would look with different color eyes.

10. Alcon has placed the Website into the stream of commerce as evinced by its social media presence and various advertising.

11. The technology utilizes a camera to “virtually try-on” contact lenses, by scanning a potential customer’s face, identifying the potential customers’ retina, iris, and/or facial geometry, and then allowing that potential customer to “try on” various contact lens colors on the potential customers’ face as shown in the picture on the device.



12. Alcon's "My Eye Color Studio" functions, at least in part, by scanning, collecting, storing, and using customers' or potential customers' iris and/or retinal biometrics. This exposes Defendant's customers and potential customers, including Plaintiff, to serious and irreversible privacy risks.

13. For example, if a biometric database is hacked, breached, or otherwise exposed – such as in the recent Equifax data breach – users have no means by which to prevent identity theft, unauthorized tracking, and other improper or unlawful use of this information.

14. The Illinois Biometric Information Privacy Act (hereinafter "BIPA" or the "Act") expressly obligates Defendant to obtain an executed, written release from an individual, prior to the capture, collection, and/or storage of an individual's biometric identifiers or biometric information, especially an eye scan, and biometric information derived from it. Burying a vague reference to biometric information in an online privacy policy is not sufficient to comply with BIPA's requirements.

15. BIPA further obligates Defendant to inform those who use their technology in writing that a biometric identifier or biometric information is being collected or captured; to tell its users in writing for how long it will store their biometric data or information and any purposes for which biometric information is being captured, collected, and used; and to make available a written policy disclosing when it will permanently destroy such information.

16. BIPA makes all of these requirements a *precondition* to the collection or recording of face geometry scans, or other associated biometric information. Under the Act, no biometric identifiers or biometric information may be captured, collected, purchased, or otherwise obtained if these pre-capture, pre-collection, pre-storage, or pre-obtainment requirements are not met.

17. The State of Illinois takes the privacy of biometric data seriously.

18. There is no realistic way, absent surgery, to reassign someone's biometric data. A person can obtain a new social security number, but not a new face, which makes the protection of, and control over, biometric identifiers and biometric information critical.

19. Defendant captured, collected, received through trade, and/or otherwise obtained biometric identifiers or biometric information of their Illinois users, like Plaintiff, without properly obtaining the above-described written executed release, and without making the required disclosures concerning the collection, storage, use, or destruction of biometric identifiers or information.

20. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and has not and will not destroy Plaintiff's or the Class's biometric data as required by BIPA.

21. Plaintiff and the putative Class are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the users' last interactions with the company.

22. Plaintiff seeks damages and injunctive relief for Defendant's BIPA violations, for herself and all those similarly situated.

PLAINTIFF SPECIFIC ALLEGATIONS

23. Plaintiff has, at relevant times, had their biometrics – their eye and associated information – collected, captured, and used by Defendant's technology.

24. Plaintiff used Defendant's "My Eye Color Studio" through Alcon's online retailer MyAlcon.com, among other place, at her residence in Illinois.

25. Defendant's virtual try on technology functions by collecting, capturing, and using biometrics.

26. Upon information and belief, Defendant subsequently stored Plaintiff's biometric data in its database(s) and distributed her biometric information to various third parties.

27. Each time Plaintiff used the try on feature, Defendant unlawfully collected their biometrics.

28. Plaintiff was never made aware of any publicly available BIPA policy. Further, Plaintiff was never provided the information required by BIPA from Defendant.

29. Plaintiff has never been informed of the specific limited purposes or length of time for which Defendant collected, stored, or used their biometrics.

30. Plaintiff has never been informed of any biometric data retention policy developed by Defendant, nor have they ever been informed of whether Defendant will ever permanently delete their biometrics.

31. Plaintiff has never been provided with nor ever signed a written release allowing Defendant to collect, capture, store, or otherwise obtain their retinal, iris, or any other biometrics or distribute those biometrics to any third-party.

32. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein.

33. BIPA protects users like Plaintiff and the putative Class from this precise conduct, and Defendant had no right to secure this data.

34. Through BIPA, the Illinois legislature has created a right to receive certain information prior to a retailer securing their highly personal, private and proprietary biometric data. The legislature has chosen to define the capture of biometric data without receiving this extremely critical information as an injury.

35. Pursuant to 740 ILCS 14/15(b), Plaintiff and the putative Class were entitled to receive certain information prior to Defendant securing their biometric data; namely, information advising them of the specific limited purpose(s) and length of time for which it/they collect(s), store(s), and use(s) their biometric scans and any biometrics derived therefrom; information regarding Defendant's biometric retention policy; and, a written release allowing Defendant to collect and store their private biometric data.

ILLINOIS'S STRONG STANCE ON PROTECTION OF BIOMETRIC INFORMATION

36. BIPA provides valuable privacy rights, protections, and benefits to users in Illinois.

37. For example, BIPA's requirements ensure that the environment for taking of biometrics is not forced or coerced; that individuals are freely advised that, by scanning one's iris, retina, or associated biometrics, the company is capturing, extracting, creating, and recording biometrics; that individuals can keep tabs on their biometric roadmaps (*e.g.*, who has their biometrics, for long how, and how it is being used), including after one's relationship ceases, or after the company stops storing the user's biometrics if at all; that individuals can evaluate the potential consequences of providing their biometrics; that companies must give individuals the right, and opportunity, to freely consent (or decline consent) **before taking** their biometrics; and that, if the disclosure does not say

so, the user's biometrics will not be used for any other purpose except for those approved by the user. The BIPA-required environment for the taking of biometrics provides legislatively-imposed peace for biometric subjects.

38. To this end, in passing the Biometric Information Privacy Act (hereinafter "the Act") in 2008, the Illinois General Assembly found:

- (a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.
- (b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.
- (c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.
- (d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.
- ...
- (e) The full ramifications of biometric technology are not fully known.
- (f) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

See, 740 ILCS 14/5, Legislative findings; intent.

39. The law is specifically designed to require a company that collects biometrics to meet several conditions, **before collection**, aimed, in part, at educating and protecting the person whose biometrics it is taking for its own use, and requiring signed, written consent attesting that the individual has been properly informed and has freely consented to biometrics collection.

40. The Act defines "Biometric identifier" as:

a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry...

See, 740 ILCS 14/10.

41. The Act defines “Biometric information” as:

any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

See, 740 ILCS 14/10.

42. The Act defines “Confidential and sensitive information” as:

personal information that can be used to uniquely identify an individual or an individual’s account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver’s license number, or a social security number.

See, 740 ILCS 14/10.

43. The Act defines “Private entity” as:

any individual, partnership, corporation, limited liability company, association, or other group, however organized...

See, 740 ILCS 14/10.

44. The Act defines “Written release” as:

informed written consent or, in the context of employment, a release executed by an employee as a condition of employment

See, 740 ILCS 14/10.

45. The Act requires:

A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

740 ILCS 14/15(a).

46. Additionally, the Act provides:

No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

- (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
- (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).

47. Further, the Act provides:

No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

740 ILCS 14/15(c).

48. The Act also provides:

No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

- (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
- (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
- (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
- (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d).

49. Furthermore, the Act provides:

A private entity in possession of a biometric identifier or biometric information shall:

- (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
- (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

740 ILCS 14/15(e).

50. BIPA provides statutory damages if a private entity takes an Illinois user's biometrics and invades the user's privacy by circumventing BIPA's preconditions and requirements.

51. The Act explicitly provides a private right of action for violations of the Act, and provides that a prevailing party "may recover for each violation:"

- (1) against a private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or actual damages, whichever is greater;
- (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is greater;
- (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
- (4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 ILCS 14/20.

52. In fact, BIPA requires express written consent in order to capture or collect biometrics in the first place. These formalized protections enable users to freely consent to the taking of their biometrics, if they so choose, after receiving legislatively-required information.

53. Defendant violated these clear protections of the Act, and upon information and belief, continues to violate its Illinois users' biometric privacy rights.

DEFENDANT'S BIOMETRIC SCANNING OF ILLINOIS USERS

54. Defendant's virtual try on feature functions, at least in part, by collecting, capturing, and using user's biometrics.

55. Defendant captured, collected, stored, and/or otherwise obtained users' biometrics, without following BIPA's mandates, as part of the "virtual try on."

56. Moreover, Defendant caused these biometrics to be associated with users, along with other user information.

57. Defendant has not, on information and belief, properly informed users in writing that a biometric identifier or biometric information is being captured, obtained, collected or stored; informed users in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; or obtained users' proper written consent to the capture, collection, obtainment or storage of their biometric identifier and biometric information derived from it.

58. Defendant's virtual try on feature captured, collected, stored, and/or otherwise obtained Plaintiff's biometric identifier and other biometric information regarding Plaintiff.

59. Defendant did not at any time, on information and belief:

- a. inform Plaintiff in writing (or otherwise) that a biometric identifier and biometric information was being obtained, captured, collected, and/or stored, or
- b. inform Plaintiff in writing (or otherwise) of the specific purposes and length of term for which a biometric identifier or biometric information was being collected, captured, stored, and/or used, or
- c. obtain, or attempt to obtain, Plaintiff's executed written release to have Plaintiff's biometric identifier and biometric information captured, collected, stored, or recorded.

60. Plaintiff did not provide a written release to Defendant as required by BIPA for the capture, collection, storage, obtainment, and/or use of Plaintiff's biometric identifiers and information.

61. Nor did Plaintiff know or fully understand that Defendant was collecting, capturing, and/or storing biometrics when Plaintiff were scanning Plaintiff's face; nor did Plaintiff know or could Plaintiff know all of the uses or purposes for which Plaintiff's biometrics were taken.

62. Upon information and belief, Defendant has not publicly disclosed its retention schedule and guidelines for permanently destroying user biometric identifiers and information, if such guidelines even exist.

63. Defendant, on information and belief, has no written policy, made available to the public, that discloses its retention schedule and/or guidelines for retaining and then permanently destroying biometric identifiers and information that complies with the requirements of BIPA.

64. The Illinois Legislature passed BIPA in in the wake of the bankruptcy of a company called Pay By Touch, which before its demise ran "the largest fingerprint scan system in Illinois." IL H.R. Tran. 2008 Reg. Sess. No. 276 at 249 (May 30, 2008). The bankruptcy, according to the Act's cosponsor, left "thousands of customers ... wondering what will become of their biometric ... data." *Id.*

65. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers or information, and/or data derived therefrom, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long.

66. The Pay by Touch bankruptcy highlights why conduct such as Defendant's – where individuals may be aware that they are providing biometric identifiers and information, but not aware of to whom or for what other purposes they are doing so – is dangerous.

67. Thus, BIPA is the Illinois Legislatures expression that Illinois citizens have biometric privacy rights, that BIPA is intended to protect.

68. Defendant disregarded these obligations and instead unlawfully collected, stored, and used users' biometric identifiers and information, without ever receiving the individual's informed written consent as required by BIPA.

69. Because Defendant neither published a BIPA-mandated data retention policy nor disclosed the purposes for their collection of biometric identifiers and information, Plaintiff and the putative Class have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates his or their biometric data.

70. Likewise, Plaintiff and the putative Class are not aware of how long Defendant will continue to store their biometric identifiers and information.

71. Nor is Plaintiff and the putative Class told to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a buyout, merger, or a bankruptcy.

72. By and through the actions detailed above, Defendant has not only disregard the Class' privacy rights, but it has also violated BIPA.

CLASS ALLEGATIONS

73. Plaintiff brings this action on behalf herself and pursuant to 735 ILCS 5/2-801 on behalf of a class (hereinafter the "Class") defined as follows:

All persons who had their biometric identifiers, iris, retina, facial geometry, or facial data captured, collected, or received by Defendant while residing in Illinois from five years preceding the date of filing of this action through the date a class is certified in this action.

Excluded from the class are Defendant's officers and directors, Plaintiff's counsel, and any member of the judiciary presiding over this action.

74. **Numerosity:** The exact number of class members is unknown and is not available to Plaintiff at this time, but upon information and belief, there are in excess of forty potential class members, and individual joinder in this case is impracticable. Class members can easily be identified through Defendant's records.

75. **Common Questions:** There are several questions of law and fact common to the claims of Plaintiff and the Class members, and those questions predominate over any questions that may affect individual Class members. Common questions include, but are not limited to, the following:

- a. whether Defendant has a practice of capturing or collecting users' biometrics;
- b. whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with Defendant, whichever occurs first;
- c. whether Defendant obtained an executed written release from face-scanned users before capturing, collecting, or otherwise obtaining users biometrics;
- d. whether Defendant obtained an executed written release from face-scanned users before capturing, collecting, converting, sharing, storing or using user biometrics;
- e. whether Defendant provided a writing disclosing to users the specific purposes for which the biometrics are being collected, stored, and used;
- f. whether Defendant provided a writing disclosing to face-scanned users the length of time for which the biometrics are being collected, stored, and used;
- g. whether Defendant's conduct violates BIPA;
- h. whether Defendant's conduct was negligent, reckless, or willful;
- i. whether Plaintiff and Class members are entitled to damages, and what is the proper measure of damages; and
- j. whether Plaintiff and Class members are entitled to injunctive relief.

76. **Adequacy of Representation:** Plaintiff will fairly and adequately represent and protect the interest of the class and have retained competent counsel experienced in complex litigation

and class action litigation. Plaintiff have no interests antagonistic to those of the class, and Defendant has no defenses unique to Plaintiff.

77. **Appropriateness:** Class proceedings are also superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. Even if Class members were able or willing to pursue individual litigation, a class action would still be preferable due to the fact that a multiplicity of individual actions would likely increase the expense and time of litigation given the complex legal and factual controversies presented in this Class Action Complaint. A class action, on the other hand, provides the benefits of fewer management difficulties, single adjudication, economy of scale, and comprehensive supervision before a single Court, and would result in reduced time, effort and expense for all parties and the Court, and ultimately, the uniformity of decisions.

**COUNT I – FOR DAMAGES AGAINST DEFENDANT
VIOLATION OF 740 ILCS 14/1, ET SEQ. – THE BIOMETRIC INFORMATION PRIVACY ACT
INDIVIDUALLY AND ON BEHALF OF THE CLASS**

78. Plaintiff, individually and on behalf of all others similarly situated, repeats, re-alleges, and incorporates all preceding paragraphs as if fully set forth herein.

79. BIPA is a remedial statute designed to protect Illinois users, by requiring consent and disclosures associated with the handling of biometrics, particularly in the context of biometric technology. 740 ILCS 14/5(g), 14/10, and 14/15(b)(3).

80. The Illinois Legislature’s recognition of the importance of the public policy and benefits underpinning BIPA’s enactment, and the regulation of biometrics collection, is detailed in the text of the statute itself.

81. Further, the Illinois Supreme Court, in a unanimous decision made clear that **“Compliance should not be difficult.”** *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 37 (Jan. 25, 2019).

82. Additionally, the Illinois Supreme Court has made clear that the Illinois Legislature intended to “subject[] private entities who fail to follow the statute’s requirements to **substantial potential liability**, including liquidated damages, injunctions, attorney fees, and litigation expenses **‘for each violation’ of the law** (*id.* § 20) whether or not actual damages, beyond violation of the law’s provisions, can be shown.” *Id.* at ¶ 36 (emphasis added).

83. “It is clear that the legislature intended for this provision to have substantial force.” *Id.* at ¶ 37.

84. Defendant has been and continues to be a “private entity” in possession of Plaintiff’s and others’ biometrics, and it collected, captured, or otherwise obtained their biometric identifiers and biometric information within the meaning of the Act.

85. As more fully set forth above, at relevant times Defendant collected, captured, or otherwise obtained, Plaintiff’s and other users’ biometric identifiers and biometric information based on those identifiers as defined by BIPA, 740 ILCS 14/10, through Defendant’s “My Eye Color Studio.”

86. In violation of 740 ILCS 14/15(a), Defendant failed to make such a written policy publicly available to Plaintiff and other class members.

87. In violation of 740 ILCS 14/15(b), Defendant has collected, captured, stored, and/or otherwise obtained Plaintiff’s and other class members’ biometric identifiers and biometric information, without:

- a. informing Plaintiff and the Class (including, where applicable, their legal authorized representatives), in writing, that the biometric identifiers or biometric information were being obtained, collected, captured, and/or stored;
- b. informing Plaintiff and the Class (including, where applicable, their legal authorized representatives), in writing, of the specific purpose and length of term for which the biometric identifiers or biometric information were being collected, stored, and used; and

- c. receiving a written release executed by Plaintiff and/or Class members and executed by Plaintiff and/or Class members.

88. Defendant took Plaintiff's and other class members' face scans, and knowingly caused their biometrics to be captured, collected, stored, and/or otherwise obtained without making publicly available the required policy that explains, for example, any purposes for which the biometric identifiers and information were collected, a retention schedule, and guidelines for permanently destroying biometric identifiers and information.

89. As a result of Defendant's above-described acts and omissions, Defendant has invaded the privacy of Plaintiff and the Class; it has unlawfully and coercively taken their biometrics; it has failed to provide them with information required by BIPA; it has deprived them of benefits, rights, opportunities and decisions conferred and required by the Illinois legislature via BIPA; and it illegally captured, collected, recorded, possessed, converted, and/or stored their face scans, biometrics, and property.

90. Accordingly, Defendant has violated the BIPA, and Plaintiff and the Class have been damaged and are entitled to damages available under the BIPA, including liquidated damages of \$1,000 per negligent violation, \$5,000 per willful or reckless violation, or actual damages, whichever is greater. 740 ILCS 14/20(1).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class of similarly situated individuals, prays for an Order as follows:

- A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the Class as defined herein;
- B. Designating and appointing Plaintiff as representative of the Class and Plaintiff's undersigned counsel as Class Counsel;
- C. Entering judgment in favor of Plaintiff and the Class and against Defendant;

- D. Awarding Plaintiff and the Class members liquidated damages of \$1,000 per negligent violation, \$5,000 per willful or reckless violation, or actual damages, whichever is greater, for each violation of BIPA;
- E. Awarding Plaintiff and the Class members reasonable attorneys' fees and costs incurred in this litigation; and
- F. Granting all such other and further relief as the Court deems just and appropriate.

**COUNT II – FOR INJUNCTIVE RELIEF AGAINST DEFENDANT
VIOLATION OF 740 ILCS 14/1, *ET SEQ.* – THE BIOMETRIC INFORMATION PRIVACY ACT**

91. Plaintiff, individually and on behalf of all others similarly situated, repeats, re-alleges, and incorporates all preceding paragraphs as if fully set forth herein.

92. BIPA provides for injunctive relief. 740 ILCS 14/20(4).

93. Plaintiff and other Class members are entitled to an order requiring Defendant to make disclosures consistent with the Act and enjoining further unlawful conduct.

94. First, Plaintiff seeks an order requiring Defendant to publicly disclose a written policy establishing any specific purpose and length of term for which Plaintiff and others' biometrics have been collected, captured, stored, obtained, and/or used, as well as guidelines for permanently destroying such biometrics when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first, as required by 740 ILCS 14/15(a).

95. Second, Plaintiff seek an order requiring Defendant to disclose whether Defendant has retained Plaintiff's and others' biometrics in any fashion, and if, when, and how such biometrics were permanently destroyed, consistent with BIPA.

96. Third, Plaintiff seek an order requiring Defendant going forward to obtain a written release from any individual, prior to the capture, collection, and/or storage of that individual's

biometric identifiers or biometric information, especially a biometric scan, and biometric information derived from it

97. Fourth, due to the above-described facts, and Defendant's failure to make publicly available facts demonstrating BIPA compliance as BIPA requires, Defendant should be ordered to: (i) disclose if (and if, precisely how, and to whom) it has disseminated, sold, leased, traded, or otherwise profited from Plaintiff and other face scanned users' biometrics, which is strictly prohibited under BIPA; and (ii) disclose the standard of care that it employed to store, transmit, and protect such biometrics, as provided under BIPA. 740 ILCS 14/15(c), (d), (e).

98. Fifth, Defendant should be enjoined from further BIPA non-compliance and should be ordered to remedy any BIPA compliance deficiencies forthwith.

99. Plaintiff's and other Class members' legal interests are adverse to Defendant's legal interests. There is a substantial controversy between Plaintiff and Class members and Defendant warranting equitable relief so that Plaintiff and the Class may obtain the protections that BIPA entitles them to receive.

100. Plaintiff and the Class do not know what Defendant has done (or intends to do) with their biometrics. Absent injunctive relief, Defendant is likely to continue its BIPA non-compliance and Plaintiff and other Class members will continue to be in the dark on the subject.

101. For the reasons set forth above, Plaintiff are likely to succeed on the merits of Plaintiff's claims.

102. BIPA establishes the importance, value, and sensitive nature of biometrics, along with the need to protect and control it; Plaintiff are entitled to know what Defendant has done with it as set forth above, and to an affirmation and verification that it has been or will be permanently destroyed as required by 740 ILCS 14/15(a).

103. The gravity of the harm to Plaintiff and the Class, absent equitable relief, outweighs

any harm to Defendant if such relief is granted.

104. As a result, Plaintiff requests commensurate injunctive relief.

WHEREFORE, Plaintiff, individually and on behalf of the class, pray for an Order as follows:

- A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the class defined herein;
- B. Designating and appointing Plaintiff as representatives of the class and Plaintiff's undersigned counsel as class counsel;
- C. Entering judgment in favor of Plaintiff and the class and against Defendant;
- D. Awarding Plaintiff and the class members all damages available to Plaintiff and the class available under applicable law, including statutory or liquidated damages;
- E. Providing commensurate injunctive relief for Plaintiff and class members as set forth above;
- F. Awarding Plaintiff and the Class members reasonable attorneys' fees and costs incurred in this litigation; and
- G. Granting all such other and further relief as the Court deems just and appropriate.

Respectfully submitted,

Dated: October 8, 2021

By: /s/ Brandon M. Wise
Brandon M. Wise – IL Bar # 6319580
PEIFFER WOLF CARR
KANE & CONWAY, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Ph: 314-833-4825
Email: bwise@peifferwolf.com

Aaron Siri, Esq. (*Pro Hac Vice To Be Filed*)
Mason Barney, Esq. (*Pro Hac Vice To Be Filed*)
SIRI & GLIMSTAD LLP
200 Park Avenue, 17th Floor
New York, NY 10166

Telephone: 212-532-1091

Email: aaron@sirillp.com

Email: mbarney@sirillp.com

COUNSEL FOR THE PLAINTIFF AND THE
PUTATIVE CLASS